



# Certification Report

**BSI-DSZ-CC-0690-2011**

for

**STARCOS 3.4 Health HBA C1**

from

**Giesecke & Devrient GmbH**

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn  
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111



# Deutsches IT-Sicherheitszertifikat

erteilt vom



Bundesamt für Sicherheit in der Informationstechnik

**BSI-DSZ-CC-0690-2011**

**STARCOS 3.4 Health HBA C1**

from Giesecke & Devrient GmbH  
PP Conformance: Protection Profile for Health Professional Card  
(PP-HPC) with SSCD Functionality, Version 1.10,  
17 November 2009, BSI-CC-PP-0018-V3-2009  
Functionality: PP conformant plus product specific extensions  
Common Criteria Part 2 extended  
Assurance: Common Criteria Part 3 conformant  
EAL 4 augmented by AVA\_VAN.5



Common Criteria  
Recognition  
Arrangement  
for components up to  
EAL 4



The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 21 July 2011

For the Federal Office for Information Security

Bernd Kowalski  
Head of Department

L.S.



This page is intentionally left blank.

## Preliminary Remarks

Under the BSI<sup>1</sup> Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

---

<sup>1</sup> Act on the Federal Office for Information Security (BSI-Gesetz - BSI<sup>1</sup>) of 14 August 2009, Bundesgesetzblatt I p. 2821

## Contents

A Certification.....	7
1 Specifications of the Certification Procedure.....	7
2 Recognition Agreements.....	7
2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA).....	7
2.2 International Recognition of CC – Certificates (CCRA).....	8
3 Performance of Evaluation and Certification.....	8
4 Validity of the Certification Result.....	9
5 Publication.....	9
B Certification Results.....	11
1 Executive Summary.....	12
2 Identification of the TOE.....	13
3 Security Policy.....	14
4 Assumptions and Clarification of Scope.....	15
5 Architectural Information.....	15
6 Documentation.....	16
7 IT Product Testing.....	16
7.1 Developer Tests according to ATE_FUN.....	16
7.2 Evaluator Tests.....	17
7.2.1 Independent Testing according to ATE_IND .....	17
7.2.2 Penetration Testing according to AVA_VAN.....	17
8 Evaluated Configuration.....	18
9 Results of the Evaluation.....	19
9.1 CC specific results.....	19
9.2 Results of cryptographic assessment.....	20
10 Obligations and Notes for the Usage of the TOE.....	21
11 Security Target.....	21
12 Definitions.....	22
12.1 Acronyms.....	22
12.2 Glossary.....	23
13 Bibliography.....	24
C Excerpts from the Criteria.....	27
D Annexes.....	37

## A Certification

### 1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG<sup>2</sup>
- BSI Certification Ordinance<sup>3</sup>
- BSI Schedule of Costs<sup>4</sup>
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1<sup>5</sup> [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

### 2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

#### 2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL 4 resp. E3 (basic).

The new agreement was initially signed by the national bodies of Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom.

---

<sup>2</sup> Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

<sup>3</sup> Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

<sup>4</sup> Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

<sup>5</sup> Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

Within the terms of this agreement the German Federal Office for Information Security (BSI) recognises

- for the basic recognition level certificates issued as of April 2010 by the national certification bodies of France, The Netherlands, Spain and the United Kingdom.
- for the higher recognition level in the technical domain Smart card and similar Devices certificates issued as of April 2010 by the national certification bodies of France, The Netherlands and the United Kingdom.

In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

Historically, the first SOGIS-Mutual Recognition Agreement Version 1 (ITSEC only) became initially effective in March 1998. It was extended in 1999 to include certificates based on the Common Criteria (MRA Version 2). Recognition of certificates previously issued under these older versions of the SOGIS-Mutual Recognition Agreement is being continued.

## 2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the website: <http://www.commoncriteriaportal.org>

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

This evaluation contains the component AVA\_VAN.5 that is not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL 4 components of these assurance families are relevant.

## 3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product STARCOS 3.4 Health HBA C1 has undergone the certification procedure at BSI.

The evaluation of the product STARCOS 3.4 Health HBA C1 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 17<sup>th</sup> June 2011. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)<sup>6</sup> recognised by the certification body of BSI.

---

<sup>6</sup> Information Technology Security Evaluation Facility



For this certification procedure the sponsor and applicant is: Giesecke & Devrient GmbH.

The product was developed by: Giesecke & Devrient GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

## 4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

## 5 Publication

The product STARCOS 3.4 Health HBA C1 has been included in the BSI list of the certified products, which is published regularly (see also Internet: <https://www.bsi.bund.de> and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer<sup>7</sup> of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

---

<sup>7</sup> Giesecke & Devrient GmbH  
Prinzregentenstraße 159  
81677 München

This page is intentionally left blank.

## **B Certification Results**

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

# 1 Executive Summary

The Target of Evaluation (TOE) is the STARCOS 3.4 Health HBA C1, a contact based smart card with applications for the German Health Care System according to the “Gesetz zur Modernisierung der Gesetzlichen Krankenversicherung” (GKV-Modernisierungsgesetz – GMG), the “Sozialgesetzbuch” (SGB) and the privacy legislation (“Datenschutzgesetze des Bundes und der Länder”). The TOE is intended to be used as Health Professional Card (HPC) within the German Health Care System and is therefore based on the specification documents [21], [22] and [23].

The TOE comprises a Smart Card Integrated Circuit (IC with contacts) with Smart Card Embedded Software, consisting of the STARCOS 3.4 Operating System platform and the dedicated Health Professional Card applications (HPC applications). The TOE's HPC applications are based on the STARCOS 3.4 Operating System platform. More detailed: The TOE is set-up of the components

- Integrated Circuit (IC) "Smart Card Controller P5CC052V0A with specific IC Dedicated Software" provided by NXP Semiconductors Germany GmbH and
- Smart Card Embedded Software comprising the STARCOS 3.4 Operating System platform (designed as native implementation) and the dedicated HPC applications for the German Health Care System provided by Giesecke & Devrient GmbH.

The TOE's platform and its technical functionality and inherently integrated security features are designed and developed under consideration of the specifications, standards and requirements as stated in the specifications [21], [22] and [23] respective in the Security Target [6] and [8], chapters 2.1 and 2.2.

The TOE is intended to be used as Health Professional Card (HPC) within the German Health Care System. In particular, the TOE is intended to be used as a Secure Signature-Creation Device (SSCD) for qualified electronic signatures in view of the European Directive 1999/93/EC on electronic signatures [18], the German Signature Act [19] and the German Signature Ordinance [20].

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile for Health Professional Card (PP-HPC) with SSCD Functionality, Version 1.10, 17 November 2009, BSI-CC-PP-0018-V3-2009 [7].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by AVA\_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [8], chapter 7.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionalities:

TOE Security Functionality	Addressed issue
SF_AccessControl	Access control mechanisms
SF_Management	Management mechanisms
SF_Protection	Protection mechanisms

TOE Security Functionality	Addressed issue
SF_TrustedCommunication	Trusted communication mechanisms
SF_Crypto	Cryptographic functionality

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [8], chapter 8.

The assets to be protected by the TOE are defined in the Security Target [6] and [8], chapter 4.1.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [8], chapters 4.2, 4.3 and 4.4.

This certification covers the following configurations of the TOE: STARCOS 3.4 Health HBA C1. For details refer to chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

## 2 Identification of the TOE

The Target of Evaluation (TOE) is called:

### STARCOS 3.4 Health HBA C1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/ SW	NXP P5CC052V0A Smart Card Controller with specific IC Dedicated Software	Mask Identifier: V0A	Smart card modules, ROM mask of the TOE already mounted into an ID-1 smart card
2	SW	Card Operating System STARCOS 3.4	01 07 01	Software on the smart card
3	SW	EEPROM image of STARCOS 3.4 Health HBA C1	Identifier of valid images published on the G&D website	Image on the smart card
4	DOC	Guidance Documentation STARCOS 3.4 Health HBA/SMC C1 – Main Document	Version 1.3 / 2010-10-13	Document in paper / electronic form
5	DOC	Guidance Documentation for the Initialisation Phase STARCOS 3.4 Health HBA/SMC C1	Version 1.2 / 2010-11-10	Document in paper / electronic form

No	Type	Identifier	Release	Form of Delivery
6	DOC	Guidance Documentation for the Personalisation Phase STARCOS 3.4 Health HBA/SMC C1	Version 1.2 / 2010-11-10	Document in paper / electronic form
7	DOC	Guidance Documentation for the Operational Usage Phase STARCOS 3.4 Health HBA C1	Version 1.4 / 2011-02-18	Document in paper / electronic form
8	DOC	Spezifikation Generische Applikation STARCOS 3.4 Health HBA R1	Version 1.20 / 2010-12-15	Document in paper / electronic form
9	DOC	STARCOS 3.4 SmartCard Operating System Reference Manual	Edition 09.2009	Document in paper / electronic form

Table 2: Deliverables of the TOE

Basically the life-cycle of STARCOS 3.4 Health HBA C1 consists of the development phase and the operational phase. The initialisation phase completely belongs to the operational use. The TOE will be delivered as hardware, as initialisation data and as documentation. No modifications by a third party are possible (e.g. by the party loading the initialisation data into the hardware).

For the evaluation process the whole life-cycle of the TOE was considered during evaluation as far as the developer/manufacturer of the TOE is directly involved. Any delivery of the chip modules is done via a G&D security transport or a security transport maintained by another initialiser to avoid the delivery of fake chips.

The user can identify the TOE by retrieving the following information from the TOE:

- IC manufacturer data (*Chipherstellerdaten*)
- OS version (*Betriebssystemversion*)
- Completion state (*Komplettierungsstand*) and
- Initialisation table (*Initialisierungstabelle*)

To verify the TOE's identification data and in particular the identification data of its initialisation table (and therefore also of the composite TOE), the user executes the command GET PROTOCOL DATA (see [15], chapter 3.1.2, [13], chapters 4.2.2 and 5.2.12, [14], chapter 5.2.4). The identification data of valid initialisation tables are published on the Giesecke & Devrient GmbH website <https://certificates.gi-de.com> for comparison.

### 3 Security Policy

The TOE is the composition of an IC and appropriate Smart Card Embedded Software and will be used as Health Professional Card (HPC) within the German Health Care System. The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Modification and disclosure of IC assets / Smart Card Embedded Software / application data
- Compromise / forgery / misuse of confidential user or TSF data including information leakage
- Misuse of TOE functions

- Interception of communication
- Abuse of TOE functionality (including its HPC applications)
- Malfunction due to environmental stress
- Physical attacks through the TOE interfaces
- Storage, copy and release of the signature creation data (SCD)
- Derivation of the signature creation data (SCD)
- Forgery of the DTBS-representation and the electronic signature

## 4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- Secure initialisation, personalisation and management
- Adequate usage of the TOE and IT-systems
- Generation of qualified certificates
- Authentic SSCD provided by SSCD Provision Service
- Protection of the VAD
- SCA sending the data intended to be signed
- SCA protecting the data intended to be signed
- Trusted channel
- Public key infrastructure

The Security Objectives related to the environment of the TOE's dedicated HPC applications can be found in the Protection Profile [7], chapter 4.2. See also the Security Target [6] and [8], chapter 5.2.

## 5 Architectural Information

The TOE STARCOS 3.4 Health HBA C1 is composed of the already certified NXP P5CC052V0A Smart Card Controller, the STARCOS 3.4 Operating System platform and the HPC applications from Giesecke & Devrient GmbH, see also Figure 1 in [6] and [8].

The TOE is composed of the following subsystems:

- System Library
- Runtime System
- Chip Card Commands
- Security Management
- Key Management
- File System
- Non-Volatile Memory Management

- Transport Management (Protocols)
- Secure Messaging
- Crypto Functions
- Hardware

## 6 Documentation

The evaluated documentation as outlined in Table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

## 7 IT Product Testing

The tests were performed with the composite smart card product STARCOS 3.4 Health HBA C1. The physical format of the test configuration for TOE testing was either

- a card which is usable for all automatic or non-recoverable test cases or
- a simulator which is required for all interactive test cases.

Test target categories:

- Operating system (contained in ROM code and EEPROM patch code)
- Initialisation and personalisation process (PDI and ISO)
- Applications initialised respective loaded
- Completion state:
  - Completed card: Card in usage phase (completion state "COMPLETED")
  - Uncompleted card: Card in uncompleted state (completion state "INITIAL")

### 7.1 Developer Tests according to ATE\_FUN

Developer's testing approach:

- Tests to cover all actions defined in the developer's functional specification
- One good case test and one bad case for each command defined in the developer's functional specification and executable on the TOE
- Access Rules test as part of the requirements on TSF data
- Tests covering all TSF subsystems in the TOE design

Verdict for the activity:

- All test cases in each test scenario were run successfully on this TOE version.
- The developer's testing results demonstrate that the TOE performs as expected.



## 7.2 Evaluator Tests

### 7.2.1 Independent Testing according to ATE\_IND

Subset size chosen:

- The evaluators have tested all TSFI.

TSFI subset selection criteria:

- The evaluators have chosen a subset of interfaces so that all TSF could be covered by at least one test case in order to confirm that the TOE operates as specified. The valid cases as well as invalid cases were considered.

TSFI tested:

- The evaluator tested all TSFI documented in the developer's functional specification.

Evaluator's testing approach:

- The developer performed tests of all TSF with card based tests and simulator test cases.
- The evaluator selected all tests of the developer's testing documentation for sampling due to the fact that all developer tests are implemented in scripts that can run without many manual interactions within days.

Verdict for the activity:

- During the evaluator's testing the TOE operated as specified.
- The evaluators have verified the developer's test results by executing a sample of tests in the developer's test documentation.

### 7.2.2 Penetration Testing according to AVA\_VAN

Penetration testing approach:

The evaluator used the information on potential vulnerabilities collected by the evaluator during the evaluation that should be considered in the vulnerability analysis. Hereby, the evaluator took into account the ST, guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify possible potential vulnerabilities in the TOE.

The evaluator applied the following procedure while creating a list of potential vulnerabilities applicable to the TOE in its operational environment: the raw list of vulnerabilities was checked whether there are any measures in the operational environment, either IT or non-IT, which prevent exploitation of the potential vulnerability in that operational environment. The evaluator records any reasons for exclusion of potential vulnerabilities from further consideration if the evaluator determines that the potential vulnerability is not applicable in the operational environment. Otherwise the evaluator records the potential vulnerability for further consideration.

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment the evaluator devised the attack scenarios for penetration tests in the case that those potential vulnerabilities could be exploited in the TOE's operational environment.

While doing this, also the aspects of the security architecture description were considered for penetration testing. All other evaluation input was used for the creation of the tests as

well. Specifically the test documentation provided by the developer was used to find out if there are areas of concern that should be covered by tests of the evaluation body.

The source code reviews of the provided implementation representation accompanied the development of test cases and were used to find test input. The code inspection also supported the testing activity by enabling the evaluator to verify implementation aspects that could hardly be covered by test cases.

In addition the evaluator applied tests and performed code reviews during the evaluation activity of ADV\_COMP.1 to verify the implementation of the requirements imposed by the ETR and the guidance of the underlying platform. This ensured confidence in the security of the TOE as a whole.

The primary focus for devising penetration tests was to cover all potential vulnerabilities identified as applicable in the TOE's operational environment for which an appropriate test set was devised. As result of these activities, the evaluator defined a penetration test framework and produced penetration tests to verify the vulnerabilities.

Verdict for the sub-activity:

- During the evaluator's penetration testing based on the evaluator's vulnerability analysis the TOE operated as specified.
- The vulnerabilities discussed in the evaluator's vulnerability analysis are not exploitable in the intended environment for the TOE. None of the penetration tests was successful.
- The TOE is resistant to attackers with high attack potential in the intended environment for the TOE.

## 8 Evaluated Configuration

This certification covers the following configurations of the TOE: The TOE as a Health Professional Card only features one fixed configuration, the composite smart card product STARCOS 3.4 Health HBA C1 consisting of the NXP Chip P5CC052V0A, the STARCOS 3.4 Operating System platform and the HPC applications. This configuration cannot be altered by the user and the evaluation is therefore only valid for this configuration of the TOE.

The TOE comprises the parts **TOE\_IC**, **TOE\_ES**, **TOE\_APP** and **TOE\_GD** as described in the following:

- **TOE\_IC**: Consists of the Integrated Circuitry of the HPC's chip (IC), the P5CC052V0A from NXP Semiconductors Germany GmbH, and the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software (Certification ID: BSI-DSZ-CC-0466-2008 with BSI-DSZ-CC-0466-2008-MA-01). The TOE\_IC firmware contains an RSA crypto library which is not used in this composite TOE.
- **TOE\_ES**: The IC Embedded Software, the STARCOS 3.4 Operating System platform.
- **TOE\_APP**: The HPC applications, i.e. their data structures and content.
- **TOE\_GD**: The guidance documentation delivered together with the TOE (refer to [12] to [17]).

Beyond the files for the HPC applications there may be additional files for other applications, e.g. for the Health Care System, which do not belong to the TOE. The file system part of the TOE is represented by the Guidance Documentation and the

Spezifikation Generische Applikation (see [15] and [16]) that define the TOE's file system part and outline its configurable items. The TOE may be initialised with different initialisation tables that have to be compliant to the Spezifikation Generische Applikation [16] without exceeding the CC certificate. Related to the TOE's file system part these different initialisation tables differ only in non-security relevant items (e.g. key length which can range between certain given boundaries or other parameters which can be varied). The compliance of the respective initialisation table to [16] is ensured by Giesecke & Devrient GmbH by checking the initialisation table with the so-called Smart Card Application Verifier Tool after installation of the TOE.

The identification of the TOE is described in [15], chapter 3.1.2, [13], chapters 4.2.2 and 5.2.12, [14], chapter 5.2.4. Different versions of initialisation tables may lead to the same TOE version. Therefore no fixed reference values can be provided. The valid initialisation tables are published on the Giesecke & Devrient GmbH website <https://certificates.gi-de.com> for comparison.

As indicated in chapter 2 the identification data of the TOE consist of information on the underlying chip, operating system, completion state and initialisation table. The following table shows the TOE's identification data as relevant for the TOE's certification (hexadecimal values):

Identification Data	Identifier
IC manufacturer data	04 11 05 39 00 30 30 35
Version of the operating system	47 44 00 B4 02
Completion state of the operating system	01 07 xy (first 3 bytes of 12 bytes in total)
Initialisation table	Refer to G&D's website

Table 3: TOE identification data

Please note that the usage of the TOE within the scope of this certification is limited in accordance with the validity of the used cryptographic algorithms, see chapters 10 and 9.2 of this report.

## 9 Results of the Evaluation

### 9.1 CC specific results

The Evaluation Technical Report (ETR) [9] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

- Application of CC to Integrated Circuits
- Smart Card evaluation guidance
- Application of Attack Potential to Smart Cards
- Composite product evaluation for Smart Cards and similar devices

- Functionality classes and evaluation methodology of physical and deterministic random number generators

(See [4], AIS 1, AIS 14, AIS 19, AIS 20, AIS 25, AIS 26, AIS 31, AIS 34, AIS 36, AIS 37, AIS 38.)

For RNG assessment the scheme interpretations AIS 20 and AIS 31 were used (see [4]).

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [10] was provided and approved. This document provides details of this platform evaluation that have to be considered in the course of a composite evaluation on top.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report).
- The component AVA\_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Protection Profile for Health Professional Card (PP-HPC) with SSCD Functionality, Version 1.10, 17 November 2009, BSI-CC-PP-0018-V3-2009 [10]
- For the Functionality: PP conformant plus product specific extensions  
Common Criteria Part 2 extended
- For the Assurance: Common Criteria Part 3 conformant  
EAL 4 augmented by AVA\_VAN.5

For specific evaluation results regarding the development and production environment see Annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

## 9.2 Results of cryptographic assessment

The following cryptographic algorithms are used by the TOE to enforce its security policy:

Hash functionalities:

- SHA-256 hash value calculation according to [24]

Algorithms for encryption and decryption:

- TDES (168 bit) according to [24]
- Retail-MAC (168 bit) according to [24]
- RSA 2048 bit according to [24]

Algorithms for signature generation and verification:

- RSA 2048 bit according to [24]

This holds for the following security functions:

- SF\_CRYPTO (SHA, RSA, 3TDES, RNG)

Random number generation e.g. for key generation, padding mechanisms and authentication protocols is performed by a physical and by a deterministic random number generator provided by the underlying hardware respective by the STARCOS 3.4 Operating System platform. The DRNG is rated as K4 with resistance against attack potential 'high' according to AIS 20 (see [4]). The rating for the PRNG is P2 with resistance against attack potential 'high' according to AIS 31 (see [4] and the certification report for the hardware BSI-DSZ-CC-0466-2008 with BSI-DSZ-CC-0466-2008-MA-01).

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). According to "Technische Richtlinie für die eCard-Projekte der Bundesregierung" BSI TR-03116 [24] and the "Algorithmenpapier" [25] the algorithms are suitable for encryption and decryption of HPC related data stored by the TOE or exchanged with the TOE, for authentication protocols implemented by the TOE as well as for signature generation and verification. The validity period of each algorithm is mentioned in the official catalogues [24] and [25].

## 10 Obligations and Notes for the Usage of the TOE

The documents as outlined in Table 2 and the Security Target [6] and [8] contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and Policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE shall be used. If non-certified updates or patches are available he should request the sponsor for providing a re-certification. In the meantime risk management process of the system using the TOE shall investigate and decide on the usage of not yet certified updates and patches or to take additional measures in order to maintain system security.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9.2 has to be considered by the user and his system risk management process.

In addition, the following aspects need to be fulfilled when using the TOE: Principally, the user has to follow the instructions in the user guidance documents [12] to [17] and has to ensure the fulfilment of the Assumptions about the environment in the Security Target [6] and [8]. There are no further requirements for the usage of the TOE contained in [9].

## 11 Security Target

For the purpose of publishing, the Security Target [8] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

## 12 Definitions

### 12.1 Acronyms

<b>AIS</b>	Application Notes and Interpretations of the Scheme
<b>BSI</b>	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
<b>BSIG</b>	BSI-Gesetz / Act on the Federal Office for Information Security
<b>CCRA</b>	Common Criteria Recognition Arrangement
<b>CC</b>	Common Criteria for IT Security Evaluation
<b>CEM</b>	Common Methodology for Information Technology Security Evaluation
<b>DES</b>	Data Encryption Standard
<b>DRNG</b>	Deterministic Random Number Generator
<b>DTBS</b>	Data to be signed
<b>EAL</b>	Evaluation Assurance Level
<b>eHC</b>	electronic Health Card
<b>ETR</b>	Evaluation Technical Report
<b>HPC</b>	Health Professional Card
<b>IT</b>	Information Technology
<b>ITSEC</b>	Information Technology Security Evaluation Criteria
<b>ITSEF</b>	Information Technology Security Evaluation Facility
<b>PP</b>	Protection Profile
<b>PRNG</b>	Physical Random Number Generator
<b>QES</b>	Qualified Electronic Signature
<b>RAD</b>	Reference Authentication Data
<b>RNG</b>	Random Number Generator
<b>RSA</b>	Rivest Shamir Adleman Algorithm
<b>SAR</b>	Security Assurance Requirement
<b>SCA</b>	Signature Creation Application
<b>SCD</b>	Signature Creation Data
<b>SFP</b>	Security Function Policy
<b>SFR</b>	Security Functional Requirement
<b>SHA</b>	Secure Hash Algorithm
<b>SMC</b>	Security Module Card
<b>SSCD</b>	Secure Signature-Creation Device
<b>ST</b>	Security Target
<b>SVD</b>	Signature Verification Data

<b>TOE</b>	Target of Evaluation
<b>TSF</b>	TOE Security Functionalities
<b>VAD</b>	Verification Authentication Data

## 12.2 Glossary

**Augmentation** - The addition of one or more requirement(s) to a package.

**Extension** - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

**Formal** - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

**Informal** - Expressed in natural language.

**Object** - An passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

**Protection Profile** - An implementation-independent statement of security needs for a TOE type.

**Security Target** - An implementation-dependent statement of security needs for a specific identified TOE.

**Semiformal** - Expressed in a restricted syntax language with defined semantics.

**Subject** - An active entity in the TOE that performs operations on objects.

**Target of Evaluation** - A set of software, firmware and/or hardware possibly accompanied by guidance.

**TOE Security Functionality** - combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

## 13 Bibliography

- [1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Part 1: Introduction and general model, Revision 3, July 2009  
Part 2: Security functional components, Revision 3, July 2009  
Part 3: Security assurance components, Revision 3, July 2009
- [2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009
- [3] BSI certification: Procedural Description (BSI 7125)
- [4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE<sup>8</sup>
- [5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI website
- [6] Security Target BSI-DSZ-CC-0690-2011, Version 2.0, 9<sup>th</sup> June 2011, Security Target STARCOS 3.4 Health HBA C1, Giesecke & Devrient GmbH (confidential document)
- [7] Protection Profile for Health Professional Card (PP-HPC) with SSCD Functionality, Version 1.10, 17 November 2009, BSI-CC-PP-0018-V3-2009
- [8] Security Target BSI-DSZ-CC-0690-2011, Version 2.0, 9<sup>th</sup> June 2011, Security Target Lite STARCOS 3.4 Health HBA C1, Giesecke & Devrient GmbH (sanitised public document)
- [9] Evaluation Technical Report, Version 5, 9<sup>th</sup> June 2011, Evaluation Technical Report Summary STARCOS 3.4 Health HBA C1, TÜV Informationstechnik GmbH (confidential document)
- [10] ETR for composite evaluation according to AIS 36 for the Product NXP P5CC052V0A Smart Card Controller, BSI-DSZ-CC-0466-2008 and amendment BSI-DSZ-CC-0466-2008-MA-01, Version 1.3, 29<sup>th</sup> September 2010, T-Systems GEI GmbH (confidential document)

---

<sup>8</sup>specifically

- AIS 20, Version 1, 2. December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 6, 7 September 2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 7, 3 August 2010, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 1, 25 Sept. 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 6, 3 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, 3 September 2009, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 3, 19 October 2010, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results



- [11] Configuration list for the TOE, Version 1.3, 9<sup>th</sup> June 2011, Configuration List STARCOS 3.4 Health HBA C1 (confidential document)
- [12] Guidance Documentation STARCOS 3.4 Health HBA/SMC C1 – Main Document, Version 1.3, 13<sup>th</sup> October 2010, Giesecke & Devrient GmbH
- [13] Guidance Documentation for the Initialisation Phase STARCOS 3.4 Health HBA/SMC C1, Version 1.2, 10<sup>th</sup> November 2010, Giesecke & Devrient GmbH
- [14] Guidance Documentation for the Personalisation Phase STARCOS 3.4 Health HBA/SMC C1, Version 1.2, 10<sup>th</sup> November 2010, Giesecke & Devrient GmbH
- [15] Guidance Documentation for the Operational Usage Phase STARCOS 3.4 Health HBA C1, Version 1.4, 18<sup>th</sup> February 2011, Giesecke & Devrient GmbH
- [16] Spezifikation Generische Applikation STARCOS 3.4 Health HBA R1, Version 1.20, 15<sup>th</sup> December 2010, Giesecke & Devrient GmbH
- [17] STARCOS 3.4 SmartCard Operating System Reference Manual, Edition 09.2009, Giesecke & Devrient GmbH
- [18] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures
- [19] Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) in der Fassung vom 16. Mai 2001 (BGBl. Jahrgang 2001 Teil I Nr. 22) zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091)
- [20] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) in der Fassung vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59) zuletzt geändert durch die Verordnung vom 17. Dezember 2009 (BGBl. I S. 3932)
- [21] Specification German Health Professional Card and Security Module Card - Part 1: Commands, Algorithms and Functions of the COS Platform, Version 2.3.0, 04.07.2008, BundesÄrzteKammer, Kassenärztliche Bundesvereinigung, BundesZahnÄrzteKammer, BundesPsychotherapeutenKammer, Kassenzahnärztliche Bundesvereinigung, Bundesapothekerkammer, Deutsche Krankenhaus-Gesellschaft
- [22] Specification German Health Professional Card and Security Module Card - Part 2: HPC Applications and Functions, Version 2.3.0, 04.07.2008, BundesÄrzteKammer, Kassenärztliche Bundesvereinigung, BundesZahnÄrzteKammer, BundesPsychotherapeutenKammer, Kassenzahnärztliche Bundesvereinigung, Bundesapothekerkammer, Deutsche Krankenhaus-Gesellschaft
- [23] Specification Related Questions Nr. 0001 bis 0003, 08.08.2008, BundesÄrzteKammer, Kassenärztliche Bundesvereinigung, BundesZahnÄrzteKammer, BundesPsychotherapeutenKammer, Kassenzahnärztliche Bundesvereinigung, Bundesapothekerkammer, Deutsche Krankenhaus-Gesellschaft
- [24] BSI TR-03116, Technische Richtlinie für die eCard-Projekte der Bundesregierung, Version 3.04, 11.06.2010
- [25] Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 16. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 16. November 2001, Bundesnetzagentur, 20.05.2011

This page is intentionally left blank.

## C Excerpts from the Criteria

CC Part1:

### Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

**Class APE: Protection Profile evaluation** (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

**Class ASE: Security Target evaluation** (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

### Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.”

“Each assurance class contains at least one assurance family.”

“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high- level design presentation

Assurance Class	Assurance Components	
AGD:	AGD_OPE.1 Operational user guidance	
Guidance documents	AGD_PRE.1 Preparative procedures	
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support	
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage	
	ALC_DEL.1 Delivery procedures	
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures	
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation	
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model	
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts	
	ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
		ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
		ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete		
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis	

Assurance class decomposition

## Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

### Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”



**Evaluation assurance level 1 (EAL1) - functionally tested** (chapter 8.3)

## “Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

**Evaluation assurance level 2 (EAL2) - structurally tested** (chapter 8.4)

## “Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

**Evaluation assurance level 3 (EAL3) - methodically tested and checked** (chapter 8.5)

## “Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

**Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed**  
(chapter 8.6)**“Objectives**

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

**Evaluation assurance level 5 (EAL5) - semiformally designed and tested** (chapter 8.7)**“Objectives**

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

**Evaluation assurance level 6 (EAL6) - semiformally verified design and tested**  
(chapter 8.8)**“Objectives**

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

## **Evaluation assurance level 7 (EAL7) - formally verified design and tested** (chapter 8.9)

### "Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

## **Class AVA: Vulnerability assessment** (chapter 16)

"The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE."

## **Vulnerability analysis (AVA\_VAN)** (chapter 16.1)

### "Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

This page is intentionally left blank

## **D Annexes**

### **List of annexes of this certification report**

Annex A: Security Target Lite provided within a separate document.

Annex B: Evaluation results regarding development and production environment.

This page is intentionally left blank.

## Annex B of Certification Report BSI-DSZ-CC-0690-2011

### Evaluation results regarding development and production environment



The IT product STARCOS 3.4 Health HBA C1 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 21 July 2011, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC\_CMC.4, ALC\_CMS.4, ALC\_DEL.1, ALC\_DVS.1, ALC\_LCD.1, ALC\_TAT.1)

are fulfilled for the development and production sites of the TOE listed below:

- a) Zamdorfer Straße 88, 81677 München (development)
- b) Prinzregentenstraße 159, 81677 München (system administration)

For the development and production sites regarding the "Smart Card Controller P5CC052V0A with specific IC Dedicated Software" from NXP Semiconductors Germany GmbH refer to the certification report BSI-DSZ-CC-0466-2008 and the corresponding amendment BSI-DSZ-CC-0466-2008-MA-01.

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the Threats, Security Objectives and requirements for the TOE life-cycle phases up to delivery (as stated in the Security Target [6] and [8]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.